

UNITED STATES DISTRICT COURT

for the  
Eastern District of Pennsylvania

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)  
information associated with email account address Justyn.  
p213@213@gmail.com that is stored at premises controlled  
by Google Inc

Case No. 18-303-M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A, ANNEXED TO THE AFFADAVIT OF PROBABLE CAUSE

located in the EASTERN District of PENNSYLVANIA, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B, ANNEXED TO THE AFFADAVIT OF PROBABLE CAUSE

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 USC §§ 2251(a), 2252(a)  
(1), and 2252(a)(4)

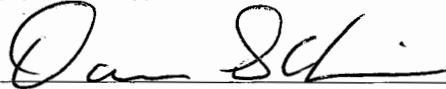
Offense Description

production of child pornography, distribution of child pornography, and possession of  
child pornography

The application is based on these facts:

SEE AFFADAVIT OF PROBABLE CAUSE

- ☐ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested  
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature


DARON SCHREIER, SA FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 2/28/18

City and state: \_\_\_\_\_



Judge's signature

MARILYN HEFFLEY, US MAGISTRATE JUDGE

Printed name and title

## AFFIDAVIT

I, Daron Schreier, being duly sworn, do hereby depose and state:

### I. BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation, and have been since January of 2006. Since August of 2006, I have been assigned to the Philadelphia Division where I have been a member of the Joint Terrorism Task Force, the Cyber squad, and most recently the Violent Crimes Against Children squad. I have received training from the FBI in the fields of international terrorism, counter-intelligence, computer crime, and the enforcement of federal child pornography laws. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

2. I make this affidavit in support of an application for a search warrant for information associated with certain Google email accounts that is stored at the premises owned, maintained, controlled, or operated by Google Inc., a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government records and other information in its possession, pertaining to the subscriber or customer operating the web sites.

3. The statements contained in this affidavit are based upon my investigation, information provided by other FBI agents and Law Enforcement officers, other personnel specially trained in the seizure and analysis of computers and electronic media, and on my experience and training as a Special Agent of the FBI.

4. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that the user of Google email account Justyn.p213@gmail.com has violated Title 18, United States Code, 2251(a) [Production of Child Pornography], 2252(a)(2) [Distribution of Child Pornography], and 2252(a)(4) [Possession of Child Pornography]. There is probable cause to believe that evidence of these crimes, as described in Attachment B, will be found in the location described in Attachment A.

### II. APPLICABLE STATUTES AND TECHNICAL TERMS

5. Title 18, United States Code, Section 2251(a), makes it a crime to knowingly use, persuade, induce, or entice a minor to engage in sexually explicit conduct; for the purpose of producing visual depictions of such conduct; and the depictions are produced using materials that had been mailed, shipped, or transported in interstate or foreign commerce.

6. Title 18, United States Code, Sections 2252(a)(2) and (b)(1) make it a crime to knowingly receive or distribute, or attempt or conspire to receive or distribute, any visual depiction, using any means or facility of interstate or foreign commerce or which has been mailed, or that has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been so shipped or transported, by any means including by computer, a visual depiction of a minor engaged in sexually explicit conduct, produced using a minor engaged in such conduct.

7. Title 18, United States Code, Section 2252(a)(4)(B) makes it a crime to knowingly possess one or more matters which contain any visual depiction of a minor engaged in sexually explicit conduct, produced using a minor engaged in such conduct, that has been mailed or that has been transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or were produced using materials that were mailed or so transported, by any means including by computer.

8. Title 18 United States Code, Section 2256(2)(A) defines "sexually explicit conduct" as actual or simulated: sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or the lascivious exhibition of the genitals or pubic area of any person.

### III. COMPUTERS AND CHILD PORNOGRAPHY

9. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these images on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls.

10. The development of computers has changed this. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage.

11. Child pornographers can now transfer photographic prints made from a film camera into a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly from a digital camera onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally hundreds of millions of computers around the world.



12. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at a very high resolution.

13. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

14. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

15. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places on the computer (e.g., temporary files or Internet Service Provider client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the computer's web cache and history files of the browser used. A forensic examiner can often recover evidence which shows that a computer contains peer to peer software, and when the computer was sharing files. Such information may be maintained indefinitely until overwritten by other data.

16. Graphic image files containing child pornography can be maintained for long periods of time on a computer. Most often the collector maintains the files purposefully. But even when the pornographic files have been deleted (due to guilt or fear of discovery), however, computer forensic experts are nonetheless often able to recover the pornographic images that were purposefully possessed at some previous time from the computer's "unallocated" or "slack" space. In addition, pornographic images can often be recovered from the temporary Internet files, or "cache" of a computer. A forensic examiner often can recover evidence suggesting whether a computer has been used to access e-mail or chat programs, and files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

#### IV. CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

17. I know based on my training and experience that most individuals who are

sexually attracted to children facilitate their sexual arousal through imagery that focuses, in part or in whole, on children. Specifically, these individuals often collect child pornography. These individuals may derive sexual gratification from actual physical contact with children as well as from fantasy involving the use of pictures or other visual depictions of children or from literature describing sexual contact with children. The overriding motivation for the collection of child pornography may be to define, fuel, and validate the collector's most cherished sexual fantasies involving children. Visual depictions may range from fully clothed depictions of children engaged in non sexual activity to nude or partially nude depictions of children engaged in sexually explicit conduct.

18. In addition to child pornography, these individuals are also highly likely to collect other paraphernalia related to their sexual interest in children. This other material is sometimes referred to as "child erotica" which is defined as any material, relating to children, that serves a sexual purpose for a given individual. It is broader and more encompassing than child pornography, but at the same time the possession of such corroborative material, depending on the context in which it is found, may be behaviorally consistent with the offender's orientation toward children and indicative of his intent. It includes things such as fantasy writings, letters, diaries, drawings, cartoons and non-sexually explicit visual images of children.

19. Child pornography collectors reinforce their fantasies, often by taking progressive, overt steps aimed at turning the fantasy into reality in some or all of the following ways: collecting and organizing their child related material; masturbating while viewing the child pornography; engaging children, online and elsewhere, in conversations, sometimes sexually explicit conversations, to fuel and fortify the fantasy; interacting, both directly and indirectly, with other likeminded adults through membership in organizations catering to their sexual preference for children thereby providing a sense of acceptance and validation within a community; gravitating to employment, activities and/or relationships which provide access or proximity to children; and frequently persisting in the criminal conduct even when they have reason to believe the conduct has come to the attention of law enforcement. These are need-driven behaviors to which the offender is willing to devote considerable time, money, and energy in spite of risks and contrary to self-interest.

20. Persons with a sexual interest in children often maintain and possess their material in the privacy and security of their homes or some other secure location, such as a private office or work computer, where it is readily available. The collection may include sexually explicit or suggestive materials involving children, such as photographs, magazines, narratives, motion pictures, video tapes, books, slides, drawings, computer images, computer videos, or other visual media. Because they put so much time and energy into obtaining the material, they do not delete or destroy their collections.

21. Your affiant is also aware that those who possess child pornography often communicate and trade child pornography with other likeminded criminals over the internet or through other means.

## V. PROBABLE CAUSE

22. On February 5, 2018, an FBI Agent acting in an Undercover Capacity (hereafter referred to as Online Covert Employee or OCE) responded to Craigslist Advertisement 6476475998, which was posted in the Casual Encounters section of the Philadelphia Craigslist site. The advertisement stated, in part: "KIK crazycock213 and email me I'll send my number looking to share real incest stories fetish stories underage pedo stories I have real experiences and pictures but enjoy talkin to those about their fantasies hmu anytime Kik or email for my number and maybe we can link up". The OCE responded to the advertisement by sending a message via Kik to "crazycock213". Kik is a mobile messaging platform which allows users to have private or group chats where they can exchange text, images, or videos. Beginning on February 5, 2018, the following conversation, in part, occurred between the OCE and crazycock213:

## a. February 5, 2018:

- I. OCE: hey man, saw your post on CL looking for sick pervs. What sort of stuff you into?
- II. Crazycock213: Incest kids and a lot more

## b. February 6, 2018:

- I. OCE: same here. Boys, girls, or both? How young you like?
- II. Crazycock213: both and 1-8
- III. OCE: nice. I'm more into boys, but don't mind girls. I kinda prefer 5 and up. You got any experience
- IV. Crazycock213: I used to fuck my brother and I have two sons ima start playing with soon

## c. February 8, 2018:

- I. OCE: So how are you going to make your boys don't say anything when they're a little older?

## d. February 9, 2018:

- I. Crazycock213: haven't thought of it yet
- II. OCE: lol I need to be more like you I guess. I just need to go for it
- III. Crazycock213: So I'm staying with and old girlfriend and she has a lil girl want me to send a pick of her with my cock



IV. OCE: man, I don't want you to get caught doing anything! Have you done stuff with her before? **[No response was received to this message]**

e. February 12, 2018:

I. OCE: whatever happened with that lil girl you were staying with??

f. February 13, 2018:

I. Crazycock213: **[transmits image depicting a toddler female, approximately one a half years of age sitting on the floor in her pajamas looking up towards the camera. An adult penis is partially visible in the foreground]**

II. OCE: Shit man, that for real?? No offense, but tons of guys out there trying to pass off web pics as their own stuff. Can you send me a pic of you holding those pajamas or something?

III. Crazycock213: Yea give me a min. Her and her mom **[transmits image of what appears to be the same toddler female, sitting clothed in a chair next to an adult female. The image appears to be taken by someone sitting on the bed next to the chairs]**

IV. OCE: nice man! Sorry to doubt you, but you talk to all sort of people making shit up. You done anything with the girl yet?

V. Crazycock213: **[transmits an image depicting a close-up of the genitals of what appears to be a toddler female. An adult hand is partially visible and is pulling back what appears to be a diaper to show the genital area.]**

VI. Crazycock213: **[transmits a video which depicts what appears to be the same female toddler from the images in paragraphs N and P, sleeping on a bed wearing a pink shirt. The video depicts an unknown adult male masturbating his erect penis which is near the sleeping toddlers face.]**

23. On February 14, 2018, in response to an Administrative Subpoena issued under exigent circumstances, Craigslist provided records pertaining to Craigslist ID 6476475998. The records identified the poster's email address as Justyn.p213@gmail.com. Craigslist identified a total of 34 posts created by the user with email address Justyn.p213@gmail.com between February 19, 2017 and February 13, 2018. In numerous postings, the user identifies himself as a 23 year old male, with a height of 5'11" and weight of 250 pounds. The user also identifies his phone number in multiple advertisements, which was 267-325-6389.

24. Your affiant is aware that Craigslist utilizes an email relay server system to

provide users a level of anonymity. If an individual responds to a Craigslist advertisement via email, the email relay server system masks an individual's true email address by assigning the user a specific Craigslist email address. Any emails sent through the specific Craigslist email address are relayed to/from the user's true email address. That allows the user to log into their normal email account (for example, a Google or Yahoo account) and send an email to another Craigslist user. The recipient of the email will see that the email originated from a Craigslist email address and not the sender's true email account. In turn, any response is sent to the same Craigslist email address and then relayed automatically to the user's true email account. Therefore, any email responses or email correspondence related to the advertisements posted by Justyn.p213@gmail.com would have been relayed to/from this email account through the relay server system.

25. In addition to the advertisement described in Paragraph 23, the user of Justyn.p213@gmail.com posted other advertisements indicating an interest in child pornography or related topics:

- a. Posting ID 6307951904, posted on 09/15/2017, stated in part: "Hi this might be weird an kinky but looking to swap real incest stories with other true freaks hmu talk about everything I have true stories and want to know who else shares theses experiences"
- b. Posting ID 6353437566, posted on 10/20/2017, stated in part: "I have real incest stories and want to swap and share my experiences with other hmu to talk about things maybe we can link up and hook up hmu 267 Threetwo5 Six38nine"
- c. Posting ID 6395223482, posted on 11/20/2017, stated in part: "Looking to swap real incest story cause I have a bunch and jerk off with someone hmu by text with all you story's or if you wanna hear mine 267 Three25 Sixthree89"
- d. Posting ID 6435490764, posted on 12/29/2017, stated in part: "I'm 23 and have several real incest stories about me and my family happened over a long time and like to share my experiences with ppl that actually have too so hmu to talk whenever and we can go from there."
- e. Posting ID 6442369015, posted on 12/29/2017, stated in part: "Looking for men with particularly dark taboo taste. I have some things I like that most people find taboo and I want converse with others on suck topics email me ur interest and I'll send my number and we can text fetishes incest underage unspeakable etc. nothing off limits and I have real encounters to share"
- f. Posting ID 6443294395, posted on 12/31/2017, stated in part: "Looking for those freaks wanting to get off on third nasty desires I have real stories and pics to swap incest fetishes underage molestation fantasies hmu let's kik or I'll send my number jpc227 I have real stories and am looking for others with real stories and hardcore fantasies"



- g. Posting ID 6444032410, posted on 01/03/2018, stated in part: "I'm looking for nasty perverts to kik or text with jpc227 is my kik the darker the better I have real story's and pictures so u do too incest rape underage molestation hardcore wanna cum with other nasty pervs"
- h. Posting ID 6447336638, posted 01/04/2018, stated in part: "Looking for dirty mean who like to beat their cock to the thought of incest and rape and underage sex ect hmu in kik jpc227 or ill give u my number I got real pics n stories"
- i. Posting ID 6449693213, posted 01/05/2018, stated in part: "Looking for someone who is interested in helping me breed my sons if interested kik me and find out more jpc227"
- j. Posting ID 6474329398, posted 01/26/2018, stated in part: "Looking for sick pervs who like incest dirty kinks under age pedo nasty shit I have real pics and real stories to trade email me and I'll send my number waiting to get off maybe make a play day with me and my sons. For more info hmu this is real KIK crazycock213"

26. A search of the Accurant law enforcement database for telephone number 267-325-6389 found that it was a wireless number affiliated with JUSTYN PEREZ COLON, 2216 N. Bouvier Street, Philadelphia, PA 19132, between October 2013 and February 2018. A search in the Accurant database for the above described individual at this address resulted in a hit for a JUSTYN PEREZ COLON (a.k.a. JUSTYN PEREZ, JUSTYN COLON) with a date of birth of February 12, 1994 and a social security number of XXX-XX-1848. A search of Pennsylvania State records identified a mugshot photograph for a JUSTYN PEREZ-COLON, social security number XXX-XX-1848, taken on February 6, 2014. According to the records, at that time PEREZ-COLON was 19 years of age at the time, was 5'11", and weighed 280 pounds.

27. On February 14, 2018, pursuant to an Administrative Subpoena issued under exigent circumstances, Kik provided records pertaining to user "crazycock213". The records showed that the user registered the account on January 26, 2018 from an iPhone. IP login records for the time period of February 8, 2018 to February 14, 2018 showed consistent login activity from IP address 96.83.255.53. A check of the American Registry for Internet Numbers ([www.arin.net](http://www.arin.net)), found that IP address 96.83.255.53 is assigned to Comcast.

28. On February 14, 2018, pursuant to an Emergency Disclosure Request, Comcast provided records pertaining to IP address 96.83.255.53 as assigned between February 8, 2018 and February 14, 2018. The subscriber was identified as the Days Inn Horsham, 245 Easton Road, Horsham, Pennsylvania.

29. On February 14, 2018, your affiant went to the Days Inn Horsham and showed the mugshot photograph of PEREZ-COLON described above, and sanitized images of the toddler female and the adult female identified as her mother. A Days Inn employee positively identified all three as having stayed at the hotel for approximately the last five nights. The employee pulled room records which showed their room was rented to a female with a Pennsylvania

Driver's License in the name of K.M.S. The employee indicated that the group had checked out and back into the hotel three times over the last five days, and was due to check out again that morning. The employee provided a room key for K.M.S's room, which was 301. Agents made entry into room 301 at approximately 11:00am and found that it was unoccupied and appeared to have been checked out.

30. A search of Facebook for K.M.S resulted in a positive hit. Photographs within the profile were compared to K.M.S's Driver's License photograph provided by Days Inn and the image transmitted to the OCE. The photographs appeared to depict the same individual. The Facebook profile for K.M.S listed her employer as a business in Willow Grove, Pennsylvania.

31. Your affiant went to the business in Willow Grove, Pennsylvania. An employee at this location positively identified K.M.S as current employee, but advised she was working that day at the location in Doylestown, Pennsylvania. Your affiant then went to the Doylestown location, where K.M.S was located and interviewed. During the interview she provided the following information:

- a. For the last five or six days, she has been staying at the Days Inn in Horsham PA with her ex-boyfriend PEREZ-COLON and her daughter. She was doing PEREZ-COLON a favor because he was homeless and looking to get back on his feet. No one else stayed with them at the hotel.
- b. K.M.S. was shown the mugshot photograph of PEREZ-COLON and positively identified him as the male she was with at the Days Inn in Horsham. K.M.S. was shown the sanitized image of the toddler female transmitted to the OCE, which she positively identified as her daughter R.S., and provided her date of birth as September 6, 2016. K.M.S. was shown the image of the adult female sitting in a chair which was transmitted to the OCE and positively identified the female as herself.
- c. K.M.S. had no knowledge that PEREZ-COLON was taking pictures of her daughter. She did not leave her daughter alone with PEREZ-COLON except when she was showering. K.M.S verbally consented to the search of her cellphone, which revealed no sexually explicit images or videos of her daughter, and no indication of the use of the Kik application.
- d. At the time of the interview, toddler female R.S. was safely in her daycare, and the whereabouts of PEREZ-COLON were unknown. K.M.S agreed to cooperate and help the FBI locate PEREZ-COLON. K.M.S began exchanging text messages with PEREZ-COLON in the presence of your affiant. During the exchange, PEREZ-COLON indicated he was at the Burger King at Front and Olney Streets in Philadelphia. Thereafter, he began walking to a nearby train station, with his destination intending to be his mother's house in the Port Richmond neighborhood in Philadelphia

32. Based on the information described above, your Affiant instructed Agents in the vicinity of Front and Olney in Philadelphia to take PEREZ-COLON into custody based on probable cause that he had produced child pornography in violation of Title 18 USC 2251(a) and distributed child pornography in violation of Title 18 USC 2252(a). Agents in the vicinity of 11<sup>th</sup> and Olney in Philadelphia observed a male fitting the physical description of PEREZ-COLON and took him into a custody. Agents found a Pennsylvania Driver's License in the male's possession which identified him as JUSTYN MICHAEL PEREZ-COLON, date of birth February 12, 1994. Thereafter, PEREZ-COLON was transported to the Federal Building in Philadelphia.

33. While at the Federal Building, PEREZ-COLON was read his Miranda Rights and agreed to answer Agents questions. PEREZ-COLON admitted the following:

- a. He had been staying at the Days Inn in Horsham with K.M.S. and her daughter for the last five or six days. No one else stayed with them or visited them during this time.
- b. PEREZ-COLON uses the Kik account "crazycock213" on his Apple iPhone.
- c. PEREZ-COLON took multiple sexually explicit photographs and videos of toddler female R.D. within the last few days, to include the pictures and video described in the above paragraphs. These photographs and videos were taken at the Days Inn with his Apple iPhone.
- d. PEREZ-COLON distributed some or all of these files to four individuals. He distributed the files to three individual via Kik using his Apple iPhone, and distributed the files via text message on his Samsung cellphone.
- e. PEREZ-COLON used Craigslist to meet the individuals he later distributed the produced child pornography files to.

34. On February 15, 2018, United States Magistrate Judge Elizabeth T. Hey, Eastern District of Pennsylvania, signed Criminal Complaint 18-218, which charged PEREZ-COLON with violations of Title 18 USC 2251(a) [Production of Child Pornography] and USC 2252(a)(2) [Distribution of Child Pornography].

## VI. AUTHORITY TO SEARCH GOOGLE AND METHOD OF SEARCH

35. Under 18 U.S.C. §§ 2711(3) and 3127, this Court has the authority to issue the warrant directing Google Inc. to comply even though Google Inc. is not located in this district, because the Court has jurisdiction over the offense being investigated. 1.

---

1 It is possible that Google stores some portion of the information sought outside of the United States. In Microsoft Corp. v. United States, 2016 WL 3770056 (2nd Cir. 2016), the Second Circuit held that the government cannot enforce a warrant under the Stored Communications Act to require a provider to disclose records in its custody and control that are stored outside the



36. Pursuant to 18 U.S.C. §§ 2703(g), a law enforcement officer does not have to be present for either the service or execution of the warrant. It is sufficient to serve it by fax, mail, or electronically upon Google Inc.

37. I request that Google Inc. be required to produce the electronic communications and other information identified in Attachment B hereto. Because Google Inc. is not aware of the facts of the investigation, its employees are not in a position to search for relevant evidence. In addition, requiring Google Inc. to perform the search would be a burden upon the company. If Google Inc. is asked to produce all the files in the account, an employee can do that easily. Requiring Google Inc. to search the materials to determine what content is relevant would add to their burden.

38. I request that the Court authorize law enforcement agents to seize only those

---

United States. As the Second Circuit decision is not binding on this court, I respectfully request that this warrant apply to all responsive information—including data stored outside the United States—pertaining to the identified account that is in the possession, custody, or control of Google. The government also seeks the disclosure of the physical location or locations where the information is stored. Assistant United States Attorney Michelle Rotella informs me that the *Microsoft* decision is inconsistent with Third Circuit law, which holds that if a court has jurisdiction over a person or entity, it can compel the production of records, regardless of where the records are stored. *Hay Grp., Inc. v E.B.S. Acquisition Corp.*, 360 F.3d 404, 412-13 (3d Cir. 2004) (Alito, J.) (explaining that Rule 45 subpoenas can reach records beyond the territorial jurisdiction of the court when the records are controlled by someone who is subject to the court's jurisdiction):

“Paragraph (a)(2) makes clear that the person subject to the subpoena is required to produce materials in that person's control *whether or not the materials are located within the District or territory within which the subpoena can be served.*” Fed.R.Civ.Proc. 45, Committee Notes, 1991 Amendment Subdivision (a) (emphasis added); *see also* 9 JAMES WM. MOORE ET AL., MOORE'S FEDERAL PRACTICE para. 45.03 (3d ed. 2000) (“The subpoena should issue from the Court where the production of documents is to occur, regardless of where the documents are located.”); 9A CHARLES ALAN WRIGHT AND ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 2456 at 31 (1995 & 2003 Supp) (“Even records kept beyond the territorial jurisdiction of the district court issuing the subpoena may be covered if they are controlled by someone subject to the court's jurisdiction.”). Con'td....

*See also In re Auto Refinishing Paint Antitrust Litig.*, 229 F.R.D. 482, 484, 487-95 (E.D. Pa. 2005) (Padova, J.) (explaining that, even though all of the documents requested from a trade association headquartered in Belgium were also located in Belgium, the subpoena did not exceed the territorial limitations of Rule 45 because the association's leader was properly served with the subpoena while he was in the district.).

items identified in Attachment B from what is produced by Google Inc. pursuant to the search warrant. In reviewing the items, I will treat them in the same way as if I were searching a file cabinet for certain documents. Content will be scanned quickly to determine if they are relevant to my search. If they are, they will be read. If I determine that they are not relevant, I will put them aside without reading them in full. This method is similar to what a law enforcement officer would do in the search of a filing cabinet or a seized computer.

39. Under 18 U.S.C. §§ 2703(b)(1)(A), notice to the customer or subscriber is not required when the government obtains the contents of electronic communications using a search warrant.

40. I also ask that the warrant direct Google Inc. to produce identifying information pertaining to this account. The government may obtain such records by either filing a motion under 18 U.S.C. § 2703(d), or by means of a search warrant under 18 U.S.C. § 2703(c)(1)(A). Since I need a search warrant to obtain the electronic communications in any event, I am requesting account identifying information by search warrant as well. The facts set forth above show probable cause also constitute specific and articulable facts, showing that there are reasonable grounds to believe that the records and other information sought are relevant and material to an ongoing criminal investigation, as required by 18 U.S.C. § 2703(d).g.

#### VII. REQUEST TO SEAL AND FOR NONDISCLOSURE ORDER

41. It is further request that this Court issue an order sealing, until further order of this Court, all papers in support of this Application, including the Application, Affidavit, Attachments, and Search Warrant, and the requisite inventory. Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and premature disclosure of the contents of this Affidavit and related documents may have a negative impact on this continuing investigation and may jeopardize its effectiveness.

42. I further request, pursuant to 18 U.S.C. § 2705(b), that this Court direct Google Inc. not to notify any other person of this warrant until such time as the Court unseals it.

#### VIII. REQUEST FOR PRODUCTION OF RECORDS

43. The United States requests that, notwithstanding Title 18, United States Code 2252(A), Google, Inc. shall be ordered to disclose responsive data, if any, by delivering encrypted files through the Google, Inc. Law Enforcement Request System.

IX. CONCLUSION

44. Based on the facts set forth above, I have probable cause to believe that evidence of violations of 18 U.S.C. 2251(a), 2252(a)(2), and 2252(a)(4), further described in Attachment B, will be found in the Google Inc. accounts to be searched, further described in Attachment A. I therefore respectfully request the issuance of a search warrant



---

Daron Schreier  
Special Agent  
Federal Bureau of Investigation

Sworn to me this 28<sup>th</sup>  
day of February 2018.



---

HONORABLE MARILYN HEFFLEY  
United States Magistrate Judge



**ATTACHMENT A**  
**PROPERTY TO BE SEARCHED**

This warrant applies to information associated with the Google Inc. account associated with email address Justyn.p213@gmail.com that are stored at premises owned, maintained, controlled, or operated by Google Inc., a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

**ATTACHMENT B**  
**PARTICULAR THINGS TO BE SEIZED**

**I. Information to be disclosed by Google Inc.**

1. INFORMATION TO BE PROVIDED BY GOOGLE INC: For the accounts associated with email address Justyn.p213@gmail.com:
  - (a) All contact information, including full name, user identification number, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;
  - (b) All communications and messages made or received by the user to include e-mails (read, sent, deleted, draft, and unopened) whether in a mailbox, user created folders, or other storage locations, attachments, documents, graphics, and any other uploaded, saved, or associated files, including all messages in Hangouts or Voice;
  - (c) All IP logs, including all records of the IP addresses that logged into the account;
  - (d) The length of service (including start date), the types of service utilized by the user, and the means and source of any payments associated with the service (including any credit card or bank account number);
  - (e) All privacy settings and other account settings;
  - (f) All records pertaining to communications between Google Inc. and any person regarding the user or the user's Google Inc. account, including contacts with support services and records of actions taken.
  - (g) Records related to electronic devices associated or linked to the user accounts, to include cellular telephones, tablets, computers or other internet ready devices.
  - (h) Notwithstanding Title 18, United States Code, Sections 2252 and 2252A, Google shall disclose responsive data, if any, by delivering encrypted files through Google's Law Enforcement Request System (LERS).

**II. Information to be seized by the government**

- (a) All files, documents, communications, images, videos, and contacts associated with the Google account Justyn.p213@gmail.com related to visual depictions of minors engaging in sexually explicit conduct or child pornography, in violation of Title 18 U.S.C. Sections 2251, 2252(a)(2) and 2252(a)(4), along with any evidence that would tend to show the true identities of the persons committing these offenses.
- (b) All activity logs and IP logs, including all records of the IP addresses that logged into the account.

- (c) All account information, including:
  - a. All account information, including: full name, user identification number, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, services and apps used, downloaded, or purchased, and other personal identifiers; buddy lists, contacts, and address books;
  - b. The length of service (including start date), the types of service utilized by the user, and the means and source of any payments associated with the service (including any credit card or bank account number);
  - c. All privacy settings and other account settings;
  - d. All registered devices and accompanying serial numbers and other identifying numbers to include dates of activation, registration, deactivation; and
  - e. All records pertaining to communications between Google Inc. and any person regarding the user or the user's Google accounts, including contacts with support services and records of actions taken.



**CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS  
RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)**

I, \_\_\_\_\_, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Facebook, and my official title is \_\_\_\_\_. I am a custodian of records for Google Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google Inc, and that I am the custodian of the attached records consisting of \_\_\_\_\_ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Facebook; and
- c. such records were made by Facebook as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature